(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 757 972**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 16257**

(51) Int Cl[6] : **G 06 F 12/14**, G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 31.12.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 03.07.98 Bulletin 98/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CP8 TRANSAC* — FR.

(72) **Inventeur(s) :** HAZARD MICHEL.

(73) **Titulaire(s) :** .

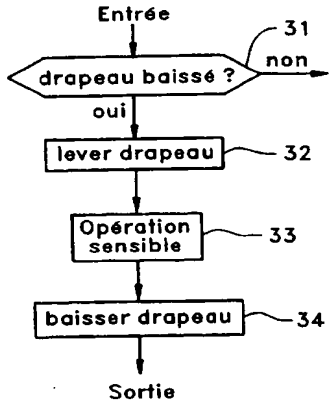
(74) **Mandataire :** BULL SA.

(54) PROCEDE DE SECURISATION D'UN MODULE DE SECURITE, ET MODULE DE SECURITE ASSOCIE.

(57) L'invention concerne un procédé de sécurisation d'un module de sécurité (8) destiné à coopérer avec un dispositif de traitement de l'information (1), le module étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible (23).

Selon l'invention, ce procédé comprend les étapes consistant à:

- exécuter, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, une première séquence supplémentaire d'opérations (32) destinée à activer des moyens de signalisation et, en aval de ladite opération sensible, une seconde séquence supplémentaire d'opérations (34) destinée à désactiver lesdits moyens de signalisation;
- vérifier, à l'occasion de chaque exécution de l'opération sensible et en amont de ladite première séquence supplémentaire d'opérations (32), si les moyens de signalisation sont désactivés;
- interdire, dans le cas où les moyens de signalisation sont activés, l'exécution de l'opération sensible.



FR 2 757 972 - A1

Procédé de sécurisation d'un module de sécurité, et module de sécurité associé

L'invention concerne un procédé de sécurisation d'un module de sécurité agencé pour coopérer avec un dispositif de traitement de l'information, le module comportant des moyens de traitement de l'information et des moyens de mémorisation de l'information et étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible. On entend, par le terme « opération sensible », toute opération dont l'exécution a des répercutions importantes sur :

- la sécurité en général : en ce qui concerne notamment toute opération visant à vérifier l'habilitation d'une personne vis-à-vis de l'accès à certaines informations, services, ou fonctions ;
- l'application concernée en particulier : en ce qui concerne notamment toute opération visant à définir ou modifier certains paramètres caractérisant les droits et obligations fondamentaux d'un usager vis-à-vis de cette application (par exemple , pour une application bancaire, une opération visant à mettre à jour un solde de compte).

Le terme "module de sécurité" doit être pris, soit dans son sens classique dans lequel il désigne un dispositif ayant vocation, dans un réseau de communication ou d'information, à être détenu par un organisme supervisant le réseau et à stocker de façon protégée des paramètres secrets et fondamentaux du réseau tels que des clés cryptographiques, soit comme désignant plus simplement un dispositif attribué à divers usagers du réseau et permettant à chacun d'eux d'avoir accès à celui-ci, ce dernier dispositif étant lui aussi susceptible de détenir des paramètres secrets. Le module de sécurité pourra prendre la forme d'un objet portatif du type carte à puce.

Le problème que vise à résoudre l'invention est d'éviter qu'une interruption de l'opération sensible en cours d'exécution ne se produise, ou du moins de contrôler le nombre d'interruptions susceptibles d'intervenir. L'invention vise tout particulièrement les interruptions frauduleuses, sans exclure toutefois les interruptions accidentelles. Le risque est que des opérations visant à sécuriser l'exécution dudit ensemble d'opérations , ne s'exécutent pas. En ce qui concerne

par exemple un programme de test d'un code confidentiel présenté par un usager, il s'agit de l'opération d'écriture du résultat de la comparaison, qui a pour but de limiter le nombre d'essais autorisés. Si le fraudeur arrive à stopper le programme après comparaison mais avant l'écriture de son résultat, il peut renouveler un grand nombre de fois l'opération de présentation d'un nouveau code confidentiel, et éventuellement tirer parti de l'observation des signaux électriques présents aux bornes du module de sécurité, signaux qui sont en pratique toujours influencés par la nature du calcul ou du résultat. Moyennant le stockage par le fraudeur d'un nombre important de telles observations et une analyse statistique, celui-ci peut éventuellement parvenir à identifier le bon code confidentiel de l'usager.

Ce problème est résolu selon l'invention en prévoyant des mesures permettant au module de sécurité de vérifier si l'opération sensible ou les opérations sensibles précédemment déclenchées ont été exécutées intégralement ou non et, dans la négative, d'interdire l'exécution de l'opération sensible à venir.

Plus précisément, le procédé selon l'invention comprend les étapes consistant à :

-exécuter, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, une première séquence supplémentaire d'opérations destinée à activer des moyens de signalisation et, en aval de ladite opération sensible, une seconde séquence supplémentaire d'opérations destinée à désactiver lesdits moyens de signalisation ;

-comptabiliser chaque essai interrompu pour lequel l'opération sensible a été déclenchée mais pas exécutée, de sorte que les moyens de signalisation ont été tout d'abord activés mais n'ont pas été ensuite désactivés, de façon à définir un nombre d'essais interrompus constaté N_{RS} ;

-définir un nombre d'essais interrompus autorisé N_{RSA} ;

-comparer, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, ledit nombre d'essais interrompus constaté N_{RS} audit nombre d'essais interrompus autorisé N_{RSA} ; et

-interdire, dans le cas où ledit nombre d'essais interrompus constaté N_{RS} est supérieur audit nombre d'essais interrompus autorisé N_{RSA}, l'exécution de l'opération sensible.

L'invention concerne aussi un module de sécurité agencé pour mettre en oeuvre ce procédé.

D'autres détails et avantages de la présente invention apparaîtront au cours de la description suivante d'un mode d'exécution préféré mais non limitatif, au regard des dessins annexés sur lesquels :

La figure 1 est le schéma d'un module de sécurité auquel est destinée l'invention, coopérant avec un dispositif de traitement de l'information ;

La figure 2 est un organigramme d'exécution d'une opération sensible ;

Les figures 3a à 3c et 4a,4b représentent l'état d'un compteur de ruptures de séquence C_{RS} à différents instants, au cours de l'exécution d'une ou plusieurs opérations sensibles ; et

La figure 5 est un organigramme d'exécution d'une opération sensible, selon une variante de l'invention.

Le dispositif de traitement de l'information 1 représenté sur la figure 1 comprend de façon connue en soi un microprocesseur 2 auquel sont reliés une mémoire ROM 3, et une mémoire RAM 4, des moyens 5 pour coopérer avec un module de sécurité 8, et une interface de transmission 7 permettant au dispositif de traitement de l'information de communiquer avec un autre dispositif semblable, soit directement, soit au travers d'un réseau de communication.

Le dispositif 1 peut en outre être équipé de moyens de stockage tels que des disquettes ou disques amovibles ou non, de moyens de saisie (tels qu'un clavier et/ou un dispositif de pointage du type souris) et de moyens d'affichage, ces différents moyens n'étant pas représentés sur la figure 1.

Le dispositif de traitement de l'information peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services, cet appareil étant installé à demeure ou portable. Il peut notamment s'agir aussi d'un appareil de télécommunications.

Par ailleurs, le module de sécurité 8 inclut des moyens de traitement de l'information 9, une mémoire non volatile associée 10, et des moyens 13 pour coopérer avec le dispositif de traitement de l'information. Ce module est agencé pour définir, dans la mémoire 10, une zone secrète 11 dans laquelle des informations une fois enregistrées, sont inaccessibles depuis l'extérieur du module mais seulement accessibles aux moyens de traitement 9, et une zone libre 12 qui est accessible depuis l'extérieur du module pour une lecture et/ou une écriture d'informations. Chaque zone de mémoire peut comprendre une partie non effaçable ROM et une partie effaçable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash", c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM classique. Une mémoire volatile RAM non représentée est par ailleurs prévue.

En tant que module de sécurité 8, on pourra notamment utiliser un microprocesseur à mémoire non volatile autoprogrammable, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Comme indiqué en page 1, ligne 5 à 17 de ce brevet, le caractère autoprogrammable de la mémoire correspond à la possibilité pour un programme fi situé dans cette mémoire, de modifier un autre programme fj situé également dans cette mémoire en un programme gj. Bien que les moyens à mettre en oeuvre pour réaliser cette autoprogrammation puissent varier selon la technique utilisée pour concevoir les moyens de traitement de l'information 9, on rappelle que, dans le cas où ces moyens de traitement sont constitués par un microprocesseur associé à une mémoire non volatile et selon le brevet précité, ces moyens peuvent inclure :

- des mémoires tampon de données et d'adresses, associées à la mémoire ;

- un programme d'écriture dans la mémoire, chargé dans celle-ci et contenant notamment les instructions permettant le maintien d'une part de la tension de programmation de la mémoire, et d'autre part des données à écrire et de leurs adresses, pendant un temps suffisant, ce programme d'écriture pouvant toutefois être remplacé par un automate d'écriture à circuits logiques.

Dans une variante, le microprocesseur du module de sécurité 8 est remplacé -ou tout du moins complété- par des circuits logiques implantés dans

une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »). A titre d'exemple, on peut citer le composant de la société SIEMENS commercialisé sous la référence SLE 4436 et celui de la société SGS-THOMSON commercialisé sous la référence ST 1335.

Avantageusement, le module de sécurité 8 sera conçu sous forme monolithique sur une seule puce.

En variante au microprocesseur à mémoire non volatile autoprogrammable décrit ci-dessus, le caractère sécuritaire du module de sécurité pourra résulter de sa localisation dans une enceinte inviolable.

Les moyens de signalisation précités comprennent au moins un compteur de ruptures de séquence C_{RS} agencé pour compter des ruptures de séquence intervenant au cours de l'exécution de l'opération sensible , c'est-à-dire des interruptions se produisant dans l'exécution , pas à pas, de cette opération. Ce compteur est incorporé aux moyens de traitement de l'information 9 du module de sécurité 8. Selon le procédé de la figure 2, on distingue deux nombres de référence, à savoir un nombre de ruptures de séquence constaté N_{RS} et un nombre de ruptures de séquence autorisé N_{RSA} , le premier correspondant au nombre de ruptures de séquence qui sont intervenues dans l'exécution d'une opération sensible déterminée depuis un instant déterminé, et le second correspondant au nombre maximum de ruptures de séquence qui peuvent intervenir sans provoquer un blocage du module de sécurité. Typiquement, l'instant à partir duquel le nombre de ruptures de séquence N_{RS} est calculé correspond à une première mise en service du module de sécurité par un utilisateur auquel celui-ci est destiné, le nombre N_{RS} comptabilisant toute rupture de séquence intervenue depuis cet instant jusqu'à un jour déterminé. Quant au nombre de ruptures de séquence autorisé N_{RSA}, il est déterminé par une autorité de façon à prendre en compte des ruptures de séquence résultant, non pas d'un

acte frauduleux, mais d'anomalies de fonctionnement du module de sécurité susceptibles d'intervenir spontanément sur toute sa durée de vie. Naturellement, N_{RSA} devra être choisi petit, faute de quoi un fraudeur bénéficierait d'un nombre confortable d'essais pour tenter de violer le module de sécurité. A titre d'exemple, N_{RSA} sera inférieur à vingt, notamment inférieur à dix.

A une entrée de l'organigramme d'exécution de l'opération sensible, une première étape 21 consiste à vérifier si le nombre de ruptures de séquence N_{RS} est bien inférieur ou égal au nombre de ruptures de séquence autorisé N_{RSA}. Dans la négative, on procède à une rupture de séquence provoquée pour interdire l'exécution de l'opération sensible : cette interruption pourra être soit définitive en ce qu'elle empêchera toute exécution ultérieure de cette opération sensible , voire en ce qu'elle bloquera tout fonctionnement ultérieur du module de sécurité , quelle que soit l'opération envisagée, soit provisoire s'il est prévu que l'opération sensible pourra être à nouveau exécutée dans l'avenir après une réinitialisation du nombre de ruptures de séquence N_{RS} par une autorité habilitée. En revanche, si le nombre de ruptures de séquence N_{RS} est bien inférieur ou égal au nombre de ruptures de séquence autorisé N_{RSA}, une seconde étape 22 consiste à incrémenter le compteur de ruptures de séquence C_{RS} d'une unité. L'étape suivante consiste à exécuter l'opération sensible elle-même. Si cette opération s'est déroulée intégralement, c'est-à-dire sans qu'une rupture de séquence accidentelle ou frauduleuse ne soit intervenue, le compteur de ruptures de séquence C_{RS} est alors décrémenté d'une unité à l'étape 24, de façon à retrouver la valeur qu'il avait avant le début de l'opération sensible.

En variante, l'opération 21 de test de la valeur du nombre de ruptures de séquence N_{RS} pourra être effectuée après celle 22 d'incrémentation du compteur de ruptures de séquence C_{RS} d'une unité.

Les figures 3a à 3c montrent des états successifs que prend le compteur de ruptures de séquence C_{RS} , en amont de l'exécution d'une opération sensible à protéger. Ce compteur est constitué par un fichier cyclique à plusieurs positions (au moins trois), chaque position étant matérialisée par au moins une cellule mémoire. Dans cet exemple, le nombre de positions est égal à huit, numérotées

de 1 à 8. Dans chaque position , est mémorisée une valeur du nombre de ruptures de séquence N_{RS} , sauf dans une position (ici la position 5) qui est vierge car ne contenant pas de valeur . Toute position vierge est repérée par le symbole Ø.

La figure 3a représente l'état du compteur en amont de l'étape 22 de l'organigramme de la figure 2. La position située au-dessus de la position vierge (ici la position 4) stocke une valeur courante N_{RS} correspondant à une valeur actuelle du compteur , tandis que les six positions 3 à 1 puis 8 à 6 stockent respectivement des valeurs différentes, prises successivement en remontant dans le temps, à savoir N_{RS} +1 pour la position 3, N_{RS} pour la position 2 ..etc..jusqu'à N_{RS} -2 pour la position 6 la plus ancienne, ces positions correspondant à un certain nombre d'opérations sensibles successives.

On peut constater que les positions 2 à 4 correspondent aux évènements suivants :

-position 2 : état du compteur avant l'étape 22 de la figure 2 ;

-position 3 : état du compteur juste après l'étape 22 (ajout d'une unité) ;

-position 4 : état du compteur juste après l'étape 24 (retrait d'un unité), ce qui montre qu'aucune rupture de séquence , volontaire ou accidentelle, n'est intervenue durant cette exécution de l'opération sensible.

En revanche, on peut constater que les positions 7 et 8 correspondent aux évènements suivants , relatifs à une exécution antérieure d'opération sensible :

-position 7 : état du compteur avant l'étape 22 de la figure 2 ;

-position 8 : état du compteur juste après l'étape 22 (ajout d'une unité) ;

-sachant que la position suivante 1 ne correspond pas à un retrait d'une unité par rapport à la position 8 (c'est-à-dire N_{RS} -1), il faut en conclure qu'une rupture de séquence , volontaire ou accidentelle, est effectivement intervenue durant cette exécution de l'opération sensible, de sorte que l'étape 24 normalement prévue n'a pas été exécutée. En conclusion, on n'a pas procédé à un nouvel enregistrement d'une valeur de compteur puisque cette valeur n'a pas changé.

Quant à la position 6, elle correspond à l'état du compteur juste avant l'étape 24, lors d'une exécution d'opération sensible encore plus ancienne. En effet, la valeur qu'elle contient correspond à celle de la position 7, augmentée d'une unité.

Revenant à l'opération sensible en cours d'exécution, la figure 3b montre l'état du compteur de ruptures de séquence dans une phase préliminaire d'exécution de l'étape 22 de l'organigramme de la figure 2. Les moyens de traitement de l'information 9 du module de sécurité ont procédé à un effacement de la position 6 située au-dessous de la position vierge 5, définissant ainsi une nouvelle position vierge. Sur la figure 3c, les moyens de traitement de l'information 9 ont exécuté l'étape 22 de la figure 2 en ajoutant une unité à la valeur courante N_{RS} de la position 4 et en stockant le résultat N_{RS} +1 dans la position suivante 5.

Les figures 4a et 4b montrent des états successifs que prend le compteur de ruptures de séquence C_{RS} , en aval de l'exécution de l'opération sensible 23 de la figure 2. La figure 4a montre l'état du compteur de ruptures de séquence dans une phase préliminaire d'exécution de l'étape 24 de la figure 2. Les moyens de traitement de l'information 9 du module de sécurité ont procédé à un effacement de la position 7 située au-dessous de la nouvelle position vierge 6. Sur la figure 4b, les moyens de traitement de l'information 9 ont exécuté l'étape 24 de la figure 2 en retranchant une unité à la valeur courante N_{RS} +1 de la position 5 et en stockant le résultat N_{RS} dans la position suivante 6.

On notera, dans l'exemple des figures 2 à 4b, que la fonction de signalisation est avantageusement imbriquée avec celle de comptage des ruptures de séquence au moyen d'un dispositif unique : le compteur de ruptures de séquence C_{RS} .

Avantageusement, les étapes 21,22 et 24 d'incrémentation et de décrémentation du compteur pourront être conçues comme des sous-programmes d'un programme principal constitué par l'opération sensible elle-même. Dans ce cas, une référence ou adresse du compteur est introduite en tant que paramètre

lors de l'appel du sous-programme. Ce mode de fonctionnement ajoute de la souplesse dans la mise en place des séquences d'opérations.

En variante au procédé de sécurisation décrit ci-dessus, la définition d'un nombre de ruptures de séquence autorisé N_{RSA} et la comptabilisation d'un nombre correspondant de ruptures de séquence constaté, pourront être supprimées si l'on estime que le module de sécurité en cause présente une fiabilité telle que la probabilité pour qu'une anomalie de fonctionnement spontanée se produise est négligeable. Un tel cas est illustré sur la figure 5. On définit, dans le module de sécurité 8, un drapeau susceptible de prendre deux états « levé » et « baissé ». Cela pourra être réalisé en pratique par une cellule mémoire pouvant prendre deux états logiques distincts. Une première étape 31 d'un organigramme d'exécution de l'opération sensible consiste à faire vérifier par les moyens de traitement de l'information 9 du module de sécurité que le drapeau est bien dans un état baissé ; si tel n'est pas le cas, il faut en conclure qu'une précédente exécution de l'opération sensible ne s'est pas effectuée complètement : en effet, on constate sur la figure 5 que toute exécution 33 de l'opération sensible se termine par une opération 34 consistant à baisser le drapeau qui a été levé en amont de l'opération sensible par une opération 32. Dans le cas où le test effectué à l'opération 31 est négatif, l'exécution de l'opération sensible est interdite ; dans le cas contraire, elle est autorisée et commence par l'exécution de l'opération de lever de drapeau 32.

Dans le cas où l'on souhaite sécuriser plusieurs opérations sensibles distinctes et destinées à être exécutées indépendemment les unes des autres, on pourra définir autant de compteurs de ruptures de séquence C_{RS} que d'opérations, chacun vérifiant la bonne exécution d'une opération sensible déterminée. Toutefois, selon un mode préféré, on ne définit qu'un seul compteur commun, qui sera incrémenté, et en principe décrémenté, lors de l'exécution d'une quelconque de ces opérations sensibles. Cette observation vaut aussi pour le cas où le compteur est remplacé par un drapeau.

Une préoccupation importante de l'invention est que la procédure de sécurisation décrite n'aboutisse pas à ralentir, voire bloquer le fonctionnement du

module de sécurité, en raison des inévitables interruptions accidentelles que l'on constate tout au long de la période de fonctionnement de celui-ci, relatives non seulement à des opérations sensibles mais aussi à des opérations ordinaires , telles que celles relatives à l'application concernée (application financière, prestation de service , etc...), dont l'inexécution n'affecte pas la sécurité en général, ni les droits et obligations fondamentaux de l'usager dans l'application concernée. En effet, le grand nombre d'opérations ainsi sécurisées risquerait de faire augmenter en conséquence le nombre d'interruptions accidentelles constatées : le nombre de ruptures de séquence autorisé N_{RSA} serait alors atteint plus rapidement, de sorte qu'un blocage partiel ou total du module de sécurité interviendrait également plus rapidement. Ce résultat remarquable est obtenu selon l'invention en n'appliquant la procédure de sécurisation décrite qu'aux opérations qui correspondent effectivement à des opérations sensibles.

Un perfectionnement de l'invention consiste en ce que le nombre d'essais interrompus autorisé N_{RSA} inclut un nombre aléatoire variant à chaque fois qu'un nombre déterminé d'opérations sensibles ont été déclenchées. Ainsi, le nombre N_{RSA} varie à une fréquence déterminée, mais il prend des valeurs successives non prévisibles, ce qui contribue à perturber toute observation frauduleuse du comportement du module de sécurité. Ce nombre aléatoire pourra être généré avantageusement dans le module de sécurité selon l'un des procédés logiciels décrits dans les brevets américains N°5.177.790 ou 5.365.466. Selon une variante, le nombre d'essais interrompus autorisé N_{RSA} est composé d'un nombre fixe auquel est ajouté un nombre aléatoire.

Revendications

1. Procédé de sécurisation d'un module de sécurité (8) agencé pour coopérer avec un dispositif de traitement de l'information (1), le module comportant des moyens de traitement de l'information (9,2) et des moyens de mémorisation de l'information (10 ; 3,4), et étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible (23) , caractérisé en ce qu'il comprend les étapes consistant à :

-exécuter, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, une première séquence supplémentaire d'opérations (22) destinée à activer des moyens de signalisation et, en aval de ladite opération sensible, une seconde séquence supplémentaire d'opérations (24) destinée à désactiver lesdits moyens de signalisation ;

-comptabiliser chaque essai interrompu pour lequel l'opération sensible a été déclenchée mais pas exécutée, de sorte que les moyens de signalisation ont été tout d'abord activés mais n'ont pas été ensuite désactivés, de façon à définir un nombre d'essais interrompus constaté N_{RS} ;

-définir un nombre d'essais interrompus autorisé N_{RSA} ;

-comparer, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, ledit nombre d'essais interrompus constaté N_{RS} audit nombre d'essais interrompus autorisé N_{RSA} ; et

-interdire, dans le cas où ledit nombre d'essais interrompus constaté N_{RS} est supérieur audit nombre d'essais interrompus autorisé N_{RSA}, l'exécution de l'opération sensible.

2. Procédé selon la revendication 1, dans lequel, pour comptabiliser chaque essai interrompu , on incrémente un compteur d'une unité à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci et, dans le cas où l'opération sensible a été exécutée, on décrémente le compteur d'une unité en aval de l'opération sensible.

3. Procédé selon la revendication 1, dans lequel ledit nombre d'essais interrompus autorisé N_{RSA} inclut un nombre aléatoire variant à chaque fois que l'opération sensible (33) a été déclenchée un nombre prédéterminé de fois.

4. Procédé de sécurisation d'un module de sécurité (8) agencé pour coopérer avec un dispositif de traitement de l'information (1), le module comportant des moyens de traitement de l'information (9,2) et des moyens de mémorisation de l'information (10 ; 3,4), et étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible (23) , caractérisé en ce qu'il comprend les étapes consistant à :

-exécuter, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, une première séquence supplémentaire d'opérations (32) destinée à activer des moyens de signalisation et, en aval de ladite opération sensible, une seconde séquence supplémentaire d'opérations (34) destinée à désactiver lesdits moyens de signalisation ;

-vérifier, à l'occasion de chaque exécution de l'opération sensible et en amont de ladite première séquence supplémentaire d'opérations (32), si les moyens de signalisation sont désactivés ;

-interdire, dans le cas où les moyens de signalisation sont activés, l'exécution de l'opération sensible.

5. Procédé selon la revendication 1 ou 4, dans lequel le module de sécurité (8) est agencé pour exécuter plusieurs opérations sensibles distinctes (33) et l'on comptabilise, au moyen du même nombre d'essais interrompus constaté N_{RS} , chaque essai interrompu relatif à l'une quelconque de ces opérations sensibles.

6. Module de sécurité (8) agencé pour coopérer avec un dispositif de traitement de l'information (1) et comportant des moyens de traitement de l'information (9,2) et des moyens de mémorisation de l'information (10 ; 3,4), et étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible (23) , caractérisé en ce qu'il comprend :

-des moyens de signalisation agencés pour prendre un état dans lequel ils sont activés en amont d'une opération sensible à protéger, et un autre état dans lequel ils sont désactivés en aval de l'opération sensible si celle-ci a été exécutée ;

-des moyens de comptage pour comptabiliser chaque essai interrompu pour lequel l'opération sensible a été déclenchée mais pas exécutée, de sorte que

les moyens de signalisation ont été tout d'abord activés mais n'ont pas été ensuite désactivés, de façon à définir un nombre d'essais interrompus constaté N_{RS}, lesdits moyens de mémorisation de l'information (10 ; 3,4) stockant un nombre d'essais interrompus autorisé N_{RSA} ;

-des moyens de comparaison pour comparer, à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci, ledit nombre d'essais interrompus constaté N_{RS} audit nombre d'essais interrompus autorisé N_{RSA} ; et

-des moyens d'interdiction pour interdire, dans le cas où ledit nombre d'essais interrompus constaté N_{RS} est supérieur audit nombre d'essais interrompus autorisé N_{RSA}, l'exécution de l'opération sensible.

7. Module de sécurité selon la revendication 6, dans lequel lesdits moyens de signalisation et de comptage comprennent un compteur agencé pour être incrémenté d'une unité à l'occasion de chaque exécution de l'opération sensible et en amont de celle-ci et, dans le cas où l'opération sensible a été exécutée, pour être décrémenté d'une unité en aval de l'opération sensible.

8. Module de sécurité (8) agencé pour coopérer avec un dispositif de traitement de l'information (1) et comportant des moyens de traitement de l'information (9,2) et des moyens de mémorisation de l'information (10 ; 3,4), et étant agencé pour exécuter un ensemble d'opérations incluant au moins une opération sensible (33) , caractérisé en ce qu'il comprend :

-des moyens de signalisation agencés pour prendre un état (32) dans lequel ils sont activés en amont d'une opération sensible à protéger, et un autre état (34) dans lequel ils sont désactivés en aval de l'opération sensible si celle-ci a été exécutée ;

-des moyens de contrôle pour contrôler, à l'occasion de chaque exécution de l'opération sensible et en amont de ladite activation (32) des moyens de signalisation, si les moyens de signalisation sont désactivés ; et

-des moyens d'interdiction pour interdire, dans le cas où les moyens de signalisation sont activés, l'exécution de l'opération sensible.

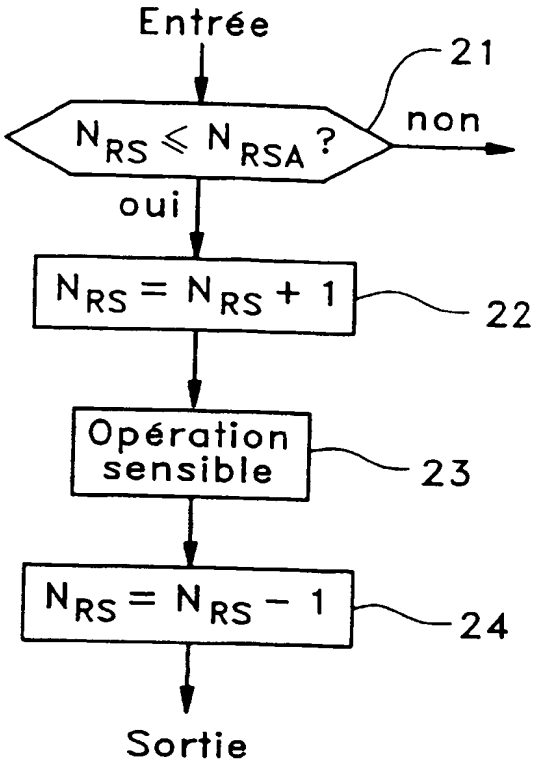


FIG.2

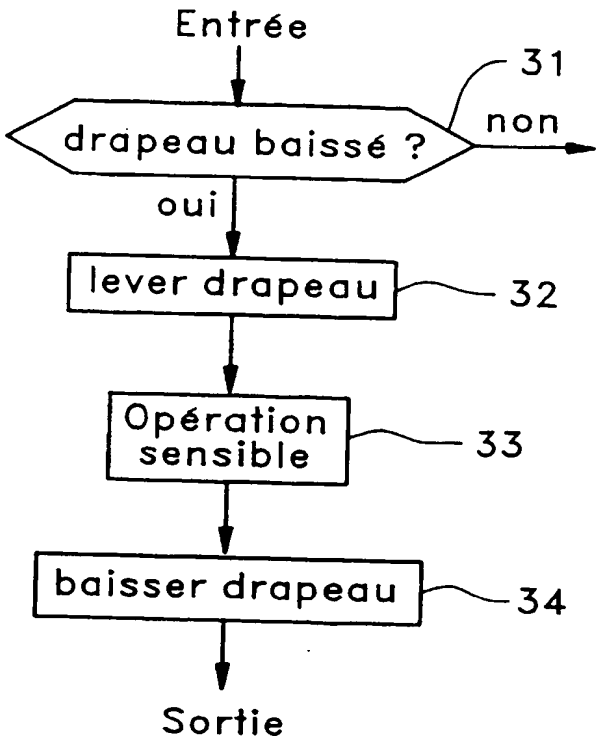


FIG.5

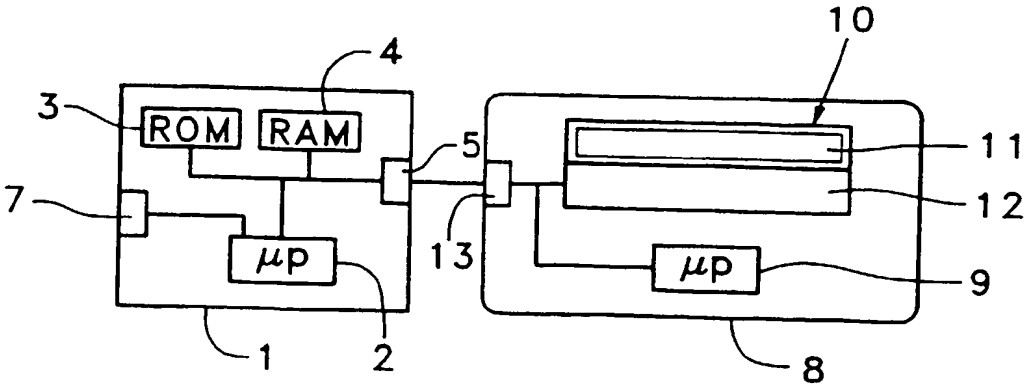


FIG.1

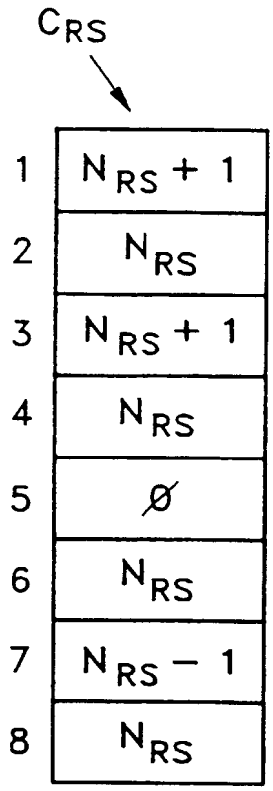


FIG.3a

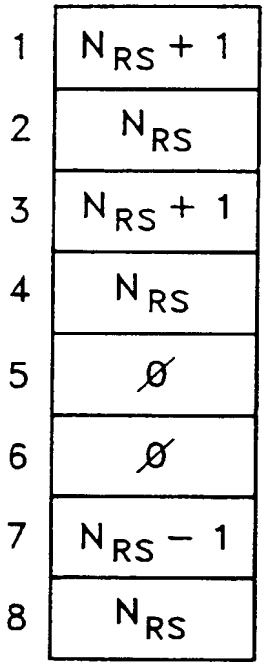


FIG.3b

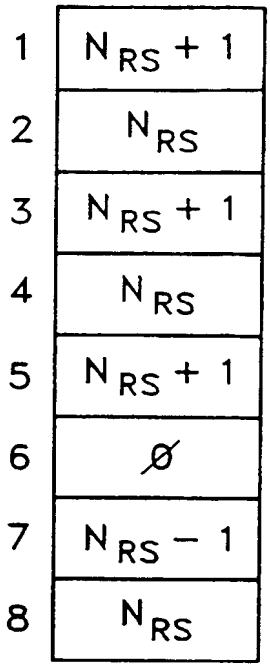


FIG.3c

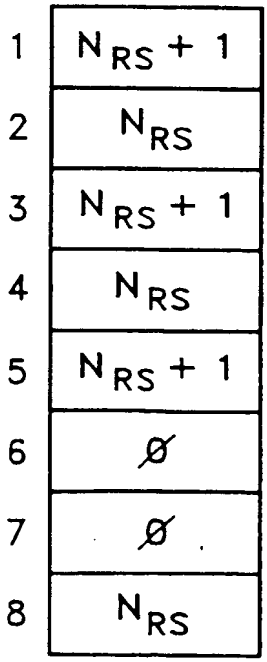


FIG.4a

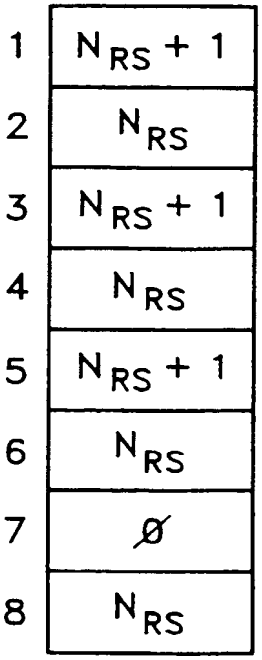


FIG.4b

2757972

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 538244
FR 9616257

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US 5 282 247 A (MCLEAN PETER T ET AL) 25 janvier 1994 * abrégé; figure 4 * * colonne 2, ligne 60 - colonne 3, ligne 38 * * colonne 9, ligne 34 - colonne 10, ligne 23 *	4,8
A	---	1,6
A	EP 0 657 820 A (SIEMENS AG) 14 juin 1995 ---	
A	EP 0 602 867 A (NCR INT INC) 22 juin 1994 ---	
A	EP 0 157 303 A (TOKYO SHIBAURA ELECTRIC CO) 9 octobre 1985 ---	
A	US 4 614 861 A (PAVLOV LEONIDAS P ET AL) 30 septembre 1986 -----	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G06F

Date d'achèvement de la recherche	Examinateur
14 octobre 1997	Powell, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)